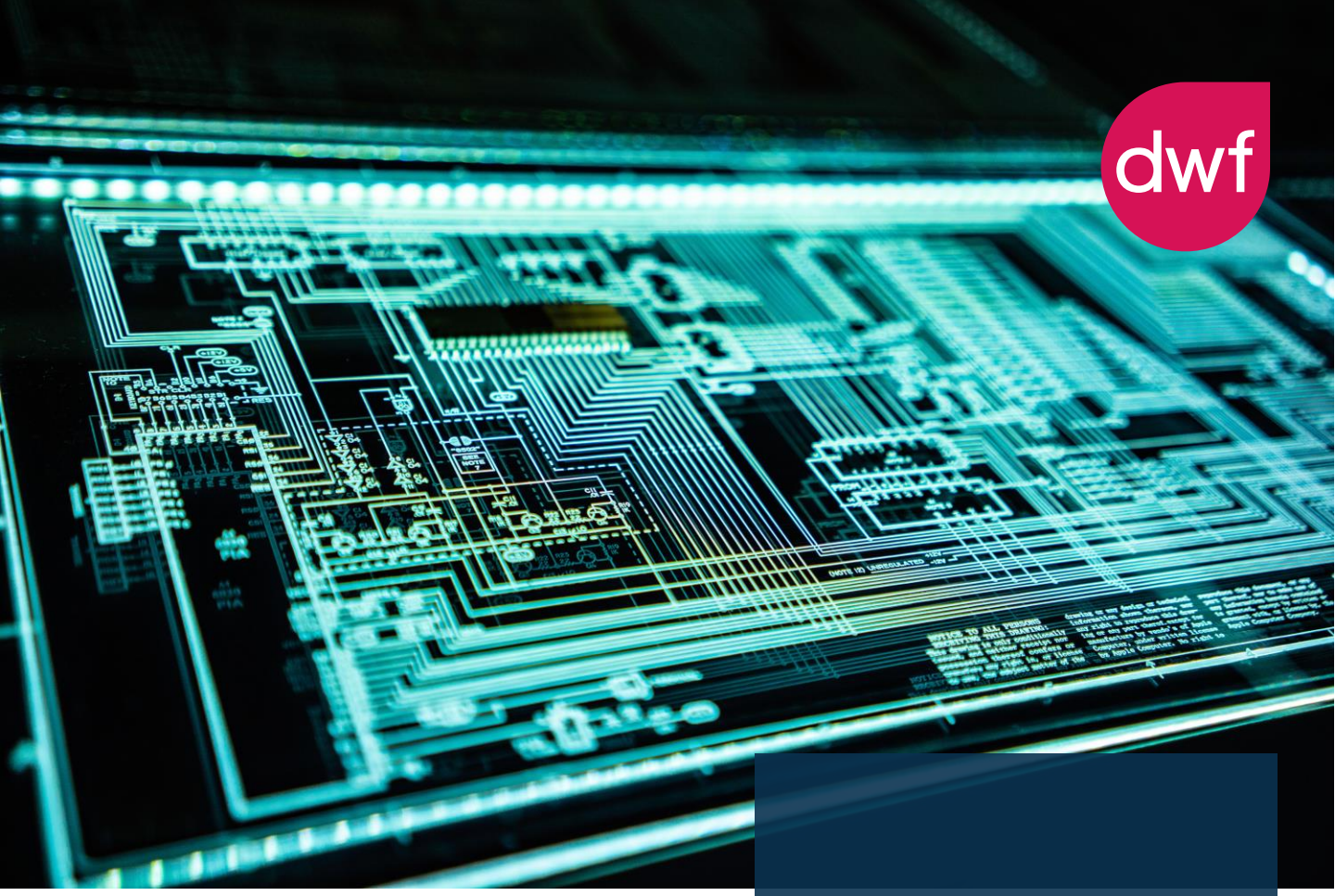


Newsletter

Tech / Data

Janvier – Février 2025

EU IA Act : publication des lignes directrices sur les pratiques interdites

La Commission Européenne publie progressivement ses lignes directrices pour une application uniforme de l'IA Act

Dans ce numéro

ACTUALITES NOUVELLES TECHNOLOGIES

Deux recommandations de la CNIL sur le développement d'une IA innovante et responsable

CNIL, recommandations pour l'information des personnes
CNIL, recommandations sur les droits des personnes

La CNIL a publié le 7 février 2025 deux recommandations afin de garantir un développement de l'intelligence artificielle (IA) conforme au Règlement général sur la protection des données (RGPD). Ces recommandations, élaborées à la suite d'une consultation publique, s'articulent autour de deux points essentiels :

- D'une part, la nécessité de renforcer l'information des personnes concernées. Les individus doivent être clairement informés lorsque leurs données personnelles sont utilisées pour entraîner un modèle d'IA. Cette information doit être accessible, transparente, et adaptée aux risques spécifiques liés à l'utilisation des données.
- D'autre part, l'importance de faciliter, pour les utilisateurs, l'exercice de leurs droits. La législation européenne propose des solutions concrètes pour permettre aux citoyens d'exercer plus facilement leurs droits, tels que le droit d'accès, la rectification ou l'opposition au traitement de leurs données. L'objectif est de garantir un meilleur contrôle des utilisateurs sur leurs informations personnelles.

La CNIL encourage également le développement d'une IA responsable et respectueuse de la vie privée. Elle recommande pour cela d'intégrer la protection des données dès la conception des modèles d'IA (privacy by design) et de mettre en place des mécanismes empêchant la divulgation de données personnelles confidentielles.

L'objectif affiché par la CNIL est de concilier innovation technologique et respect des droits fondamentaux afin de renforcer la confiance du public dans les technologies d'intelligence artificielle et assurer un déploiement responsable et éthique de l'IA.

Lignes directrices de la Commission Européenne sur les pratiques interdites en matière d'IA

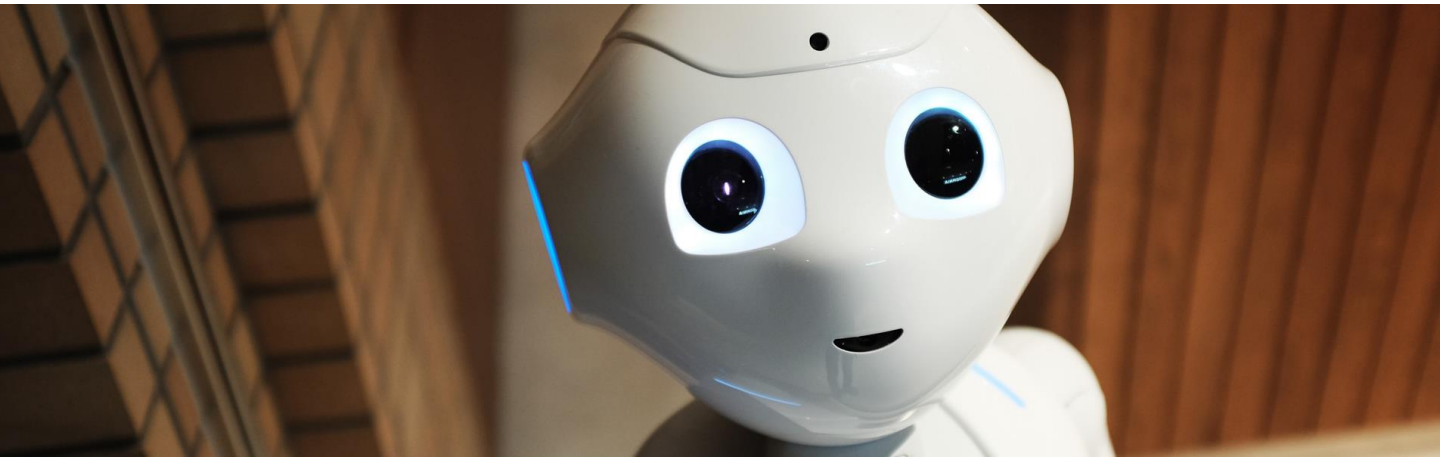
Commission Européenne, lignes directrices, 04/02/2025

La Commission européenne a publié le 4 février 2025 un projet de lignes directrices détaillant les pratiques d'intelligence artificielle (IA) jugées interdites et inacceptables en raison de leurs risques potentiels pour les valeurs européennes et les droits fondamentaux par l'IA Act. Ces lignes directrices visent à assurer une application cohérente et efficace de l'AI Act à travers l'UE, en fournissant des explications juridiques et des exemples pratiques pour aider les parties prenantes à comprendre et à se conformer aux exigences de la législation.

Ces lignes directrices se concentrent sur les pratiques interdites en matière d'IA et notamment les systèmes d'IA qui manipulent les décisions des individus ou exploitent leurs vulnérabilités, les systèmes qui évaluent ou classent les personnes en fonction de leur comportement social ou de leurs caractéristiques personnelles, menant à un traitement injustifié ou disproportionné ou encore les systèmes qui identifient les individus à distance en temps réel dans des espaces publics.

La Commission a approuvé le projet de ces lignes directrices qui doivent encore être formellement adoptées.

ACTUALITES NOUVELLES TECHNOLOGIES



Avis de la Commission européenne sur le modèle pour le résumé des données d'entraînement à fournir par les fournisseurs d'IA.

Commission européenne, avis, 17/01/2025

L'IA Act prévoit que les fournisseurs d'IA doivent mettre à disposition du public un résumé suffisamment détaillé du contenu qu'ils utilisent pour entraîner leurs modèles, afin notamment de permettre aux parties qui ont un intérêt légitime de faire valoir leurs droits. Cela vise à assurer un équilibre entre la transparence des données utilisées et la protection des secrets commerciaux des fournisseurs d'IA.

Le 17 janvier 2025, la Commission européenne a publié un avis sur le modèle à utiliser pour établir ce résumé.

Ce modèle s'applique à toutes les sources de contenus, quel que soit le stade de leur utilisation dans l'entraînement des IA. La Commission Européenne a notamment précisé que cette transparence mise en place à travers le modèle devra s'effectuer de manière simple et compréhensible pour le public en étant pour autant suffisamment détaillé pour atteindre son objectif, c'est-à-dire aider les parties ayant des intérêts légitimes à exercer leurs droits.

Le modèle se compose de trois sections. La première est relative aux informations générales, portant notamment sur le modèle d'IA et son fournisseur ou encore sur la taille, les modalités et les caractéristiques globales des données d'entraînement. La seconde est relative à la liste des sources de données (données accessibles au public, données acquises par le fournisseur...) et la troisième porte sur les autres aspects pertinents du traitement des données tels que les mesures mises en œuvre pour assurer le respect des droits de propriété littéraire et artistique ou encore celles mises en œuvre dans la suppression du contenu jugé indésirable.

Ce modèle est développé en parallèle du Code des Bonnes Pratiques dont la publication du troisième projet est attendue dans les prochains mois.

ACTUALITES NOUVELLES TECHNOLOGIES

Caducité d'un contrat de location financière de matériel informatique en cas de résiliation du contrat de maintenance.

Cass. com., 05/02/2025, n°23-23.358

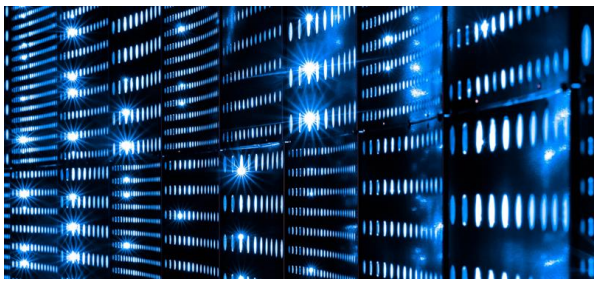
Le 5 février 2025, la chambre commerciale de la Cour de cassation a rendu un arrêt important concernant la caducité d'un contrat de location financière pour du matériel informatique.

Les sociétés Logar'Auto et Locam avaient conclu un contrat de location financière portant sur du matériel de bureautique fourni par la société Olicopie qui en assurait également la maintenance. En raison de manquements à ses obligations, Nogar'auto résilie le contrat de maintenance avec Olicopie après une mise en demeure restée infructueuse. Nogar'auto notifie ensuite à Locam la caducité du contrat de location financière, considérant que la résiliation du contrat de maintenance en justifiait la fin. Olicopie est mise en liquidation judiciaire ensuite.

Locam assigne Nogar'auto en justice afin d'obtenir le paiement des loyers impayés. Nogar'auto se défend en invoquant la caducité du contrat de location financière, en raison de la résiliation préalable du contrat de maintenance.

La Cour d'appel de Lyon rejette les arguments de la Nogar'auto relatifs à la caducité du contrat et la condamne à payer 10 335,60 euros avec intérêts.

Le 5 février 2025, au visa des articles 1186, alinéas 2 et 3, 1124, 1226 du Code civil, la Cour de cassation casse l'arrêt de la Cour d'appel de Lyon en affirmant que la résiliation du contrat de maintenance entraînait la caducité du contrat de location financière associé, sans qu'il soit nécessaire de mettre en cause le prestataire de maintenance, la société Olicopie.



Le US Copyright Office prend position sur la protection des résultats générés par l'intelligence artificielle

U.S. Copyright Office, Rapport, 29/01/2025

Le 29 janvier 2025, le US Copyright Office a publié la deuxième partie de son Rapport sur les enjeux et questions juridiques et politiques liées au droit d'auteur et à l'intelligence artificielle (IA). Cette partie du rapport traite de la possibilité de protéger par le droit d'auteur les créations générées par l'IA.

Selon ce rapport, « les principes existants concernant la législation sur le droit d'auteur sont suffisamment souples pour s'appliquer à cette nouvelle technologie », et ne nécessitent pas de modification législative spécifique à ce stade. Ainsi, le US Copyright Office réaffirme qu'une création ne pourrait être protégée par le droit d'auteur que si un auteur humain y apporte une contribution expressive significative. Ainsi, le simple fait de fournir un prompt à une IA ne suffit pas à revendiquer un droit d'auteur. Toutefois, une œuvre hybride, combinant éléments générés par IA et modifications humaines et créatives pourrait bénéficier d'une protection. Le Copyright Office prévoit cependant de mettre à jour ses directives sur l'enregistrement des œuvres intégrant de l'IA afin d'apporter davantage de clarté aux créateurs et aux entreprises.

Une troisième partie du rapport, à venir, se penchera sur un autre sujet clé : celui du recours aux œuvres protégées pour entraîner les modèles d'IA, soulevant des enjeux majeurs en matière de licences et de responsabilité juridique. Cette question suscitant des préoccupations majeures notamment quant au respect du droit d'auteur sera donc au cœur des prochains débats.

ACTUALITES NOUVELLES TECHNOLOGIES

Le refus d'interopérabilité d'une entreprise peut constituer un abus de position dominante

CJUE, 25/02/2025, C-233/23

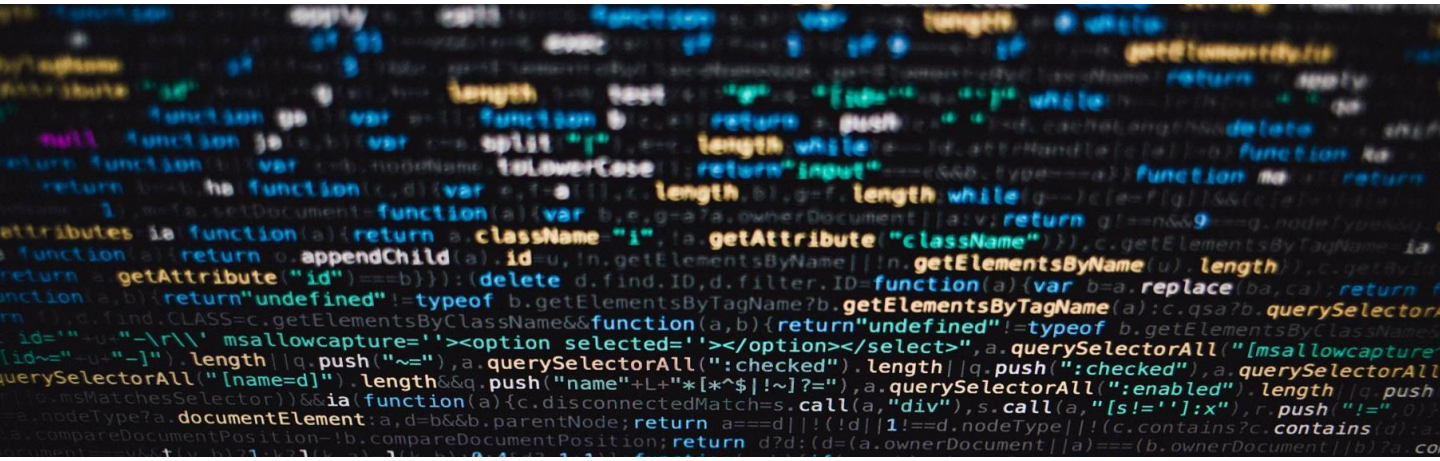
Le différend trouve son origine dans le refus de Google de rendre interopérable sa plateforme Android Auto avec l'application JuicePass, développée par Enel X Italia. Lancée en 2018 pour faciliter l'accès aux services de recharge des véhicules électriques, JuicePass devait permettre aux utilisateurs d'accéder à des bornes de recharge via une interface numérique intégrée aux systèmes d'infodivertissement des véhicules. Après plusieurs demandes de la part d'Enel X Italia, Google a invoqué des motifs de sécurité et de gestion des ressources pour refuser cette interopérabilité, réservant ainsi l'accès aux seules applications de multimédias et de messagerie.

L'AGCM (Autorità Garante della Concorrenza e del Mercato), autorité de la concurrence italienne, a sanctionné les sociétés Google, Google Italy et Alphabet pour abus de position dominante, estimant que le refus d'accès avait un effet anticoncurrentiel en favorisant indûment les services de Google, notamment son application Google Maps. La décision de l'AGCM, assortie d'une amende de plus de 102 millions d'euros, a fait l'objet d'un recours devant les juridictions italiennes, conduisant finalement le Conseil d'État italien à poser des questions préjudicielles à la CJUE concernant l'application de l'article 102 du TFUE.

Par un arrêt du 25 février 2025, la CJUE affirme que lorsqu'une entreprise en position dominante, ayant développé une plateforme numérique, refuse d'assurer l'interopérabilité de celle-ci avec une application développée par un tiers, ce refus peut être considéré comme un abus de position dominante. Cette qualification est retenue même si la plateforme n'est pas strictement indispensable à l'exploitation commerciale de l'application sur un marché en aval. En effet, si l'accès à la plateforme rend l'application plus attractive pour les consommateurs – et surtout lorsque la plateforme n'a pas été conçue exclusivement pour les besoins internes de l'entreprise dominante –, un refus peut entraver l'innovation et fausser la concurrence.

Dans cet arrêt la CJUE adapte le droit de la concurrence aux spécificités des marchés numériques. Elle cherche à garantir que les entreprises dominantes ne puissent pas bloquer l'innovation en refusant l'accès à des fonctionnalités qui, même si elles ne sont pas essentielles à l'exploitation commerciale d'une application, améliorent considérablement son attractivité pour les consommateurs. Ce cadre juridique offre ainsi un outil pour évaluer les comportements potentiellement abusifs, tout en tenant compte des réalités techniques et concurrentielles de l'environnement numérique.

ACTUALITES NOUVELLES TECHNOLOGIES



Possibilité d'obligations contractuelles renforcées des hébergeurs sur les contenus qu'ils publient ou stockent

Cass. com., 15/01/2025, n°23-14.625

Dans un arrêt du 15 janvier 2015, la chambre commerciale de la Cour de cassation a affirmé que les hébergeurs pouvaient être soumis à des obligations contractuelles renforcées en matière de contenus qu'ils publient ou qu'ils stockent.

La société Dstorage avait conclu en 2013 un contrat avec la Société Générale lui permettant d'offrir un service de paiement sécurisé par carte bancaire à ses utilisateurs. En 2015, la banque a décidé de mettre fin à cet accord après avoir constaté la présence de contenus illicites violant des droits de propriété intellectuelle sur la plateforme. La décision de résiliation était fondée sur l'article 1.4 du contrat, qui prévoyait une telle possibilité en cas d'activités illégales avérées.

Dstorage a contesté cette résiliation, soutenant qu'elle ne pouvait être tenue responsable des fichiers mis en ligne par ses utilisateurs et qu'elle avait réagi aux signalements en supprimant les contenus litigieux. L'entreprise a donc saisi la justice pour demander le rétablissement du service de paiement et l'octroi de dommages et intérêts.

Par un arrêt du 15 janvier 2025, la Cour de cassation a rejeté le pourvoi de Dstorage, confirmant la décision de la Cour d'appel de Paris du 3 mars 2023. Les juges ont ainsi estimé que l'article 6 de la Loi pour la Confiance dans l'Economie Numérique permet aux parties à un contrat d'inclure des clauses imposant aux hébergeurs une obligation de surveillance. Or, en l'espèce, Dstorage n'a pas apporté la preuve qu'elle avait mis en place des mesures techniques pour prévenir la mise en ligne récurrente de contenus illicites. La banque était donc en droit de résilier le contrat en raison des manquements constatés.

Cet arrêt illustre la volonté des juridictions françaises de responsabiliser les intermédiaires techniques dans la lutte contre la contrefaçon et les violations de la propriété intellectuelle et met en lumière la nécessité pour les plateformes numériques d'adopter des systèmes de détection et de suppression efficaces pour éviter des sanctions contractuelles pouvant impacter leur activité.

ACTUALITES DONNEES PERSONNELLES

Lignes directrices du CEPD sur la pseudonymisation et le renforcement de la coopération avec les autorités de la concurrence

CEPD, lignes directrices, 17/01/2025

Dans des lignes directrices du 17 janvier 2025, le CEPD clarifie la définition de la pseudonymisation et la manière dont elle s'applique :

- D'une part, les données pseudonymisées restent toujours des informations relatives à une personne physique identifiable. Elles constituent toujours des données personnelles.
- D'autre part, la pseudonymisation peut réduire les risques et faciliter l'utilisation de l'intérêt légitime comme base légale (article 6.1.f du RGPD), à la condition que toutes les autres exigences du RGPD soient respectées.

Ces lignes directrices ont été soumises à consultation publique jusqu'au 28 février 2025.

Le CEPD explique aussi comment la protection des données et le droit de la concurrence interagissent. Il suggère des étapes pour intégrer les facteurs de marché et de concurrence dans les pratiques de protection des données et pour que les règles de protection des données soient prises en compte dans les évaluations de la concurrence. Il fournit des recommandations pour améliorer la coopération entre les régulateurs. Ainsi, les autorités devraient envisager de créer un point de contact unique pour gérer la coordination avec d'autres régulateurs.

ACTUALITES DONNEES PERSONNELLES

Publication par la CNIL de son plan stratégique pour 2025 / 2028

CNIL, plan stratégique 2025-2028

Pour 2025/2028, la CNIL propose un plan stratégique en quatre axes :

- Promouvoir une intelligence artificielle éthique et respectueuse des droits. La popularisation de l'intelligence artificielle va de pair avec un accroissement de contenus pouvant être malveillants ou trompeurs. Face à ce constat, la CNIL poursuivra ses travaux pour clarifier et enrichir le cadre légal sur l'IA.
- Protéger les mineurs et leurs données dans l'univers numérique. Le numérique et les risques associés sont omniprésents dans le quotidien des mineurs. Face à ces enjeux, la CNIL va renforcer son dialogue avec les enfants, leur entourage et l'écosystème éducatif afin de créer un environnement numérique plus sûr.
- Faire de chacun un acteur de la cybersécurité pour renforcer la confiance dans le numérique. Ces dernières années ont été marquées par une augmentation massive des cyberattaques impliquant une grande partie de la population à travers divers secteurs tels que la santé ou le domaine bancaire. Pour lutter contre les risques de vols de données personnelles, enjeux de société majeur, la CNIL, en coopération avec l'écosystème de la cybersécurité tel l'ANSSI, s'assurera que les organismes prennent des mesures de protection adaptées et sensibilisera les individus à ces risques.
- Mettre en œuvre des actions ciblées sur des usages numériques du quotidien. La CNIL se mobilisera sur deux usages majeurs du quotidien numérique des français : les applications mobiles et la question de l'identité numérique. Concernant les applications mobiles, elle s'assurera de la conformité des acteurs et sensibilisera les utilisateurs à ses recommandations publiées en 2024. Concernant l'identité numérique, elle veillera à son développement et son déploiement par divers acteurs publics et privés, tout en s'assurant qu'elle soit à la fois conforme à la règlementation et respectueuse des droits et libertés individuels.

ACTUALITES DONNEES PERSONNELLES

Bilan de la CNIL sur ses contrôles dans le cadre d'une action coordonnée européenne

CNIL, bilan des contrôles sur le droit d'accès

Dans le cadre d'une action coordonnée européenne, la CNIL et plusieurs de ses homologues européens ont évalué la conformité et le respect des entreprises et administrations au droit d'accès aux données personnelles prévu par le RGPD.

Il en ressort que majoritairement, les entreprises et administrations ont mis en oeuvre des mesures organisationnelles afin de traiter les demandes de droit d'accès. L'enquête a cependant révélé plusieurs lacunes, notamment des retards fréquents dans les réponses aux demandes d'accès, avec de nombreuses organisations dépassant le délai d'un mois imposé par la règlementation. Certaines réponses sont également incomplètes, insuffisantes et insatisfaisantes, ne fournissant pas l'intégralité des données demandées.

Pour remédier à ces insuffisances, la CNIL recommande la mise en place de procédures internes plus efficaces, une meilleure formation des équipes concernées et une transparence accrue dans la communication des informations aux citoyens. La CNIL rappelle également l'existence des lignes directrices sur le droit d'accès adoptées par le CEPD en 2023, souvent oubliées voire méconnues, alors qu'elles comportent de précieux conseils.

En cas de non-conformité persistante, des sanctions peuvent être appliquées, la CNIL ayant déjà prononcé plusieurs rappels aux obligations légales

La CNIL publie son guide sur les analyses d'impact des transferts de données

Guide de la CNIL sur les analyses d'impact des transferts de données

Fin janvier 2025, à la suite d'une consultation publique, la CNIL a publié un guide pratique sur l'analyse d'impact des transferts de données (AITD), visant à aider les organismes transférant des données en dehors de l'Espace économique européen (EEE) à évaluer et garantir un niveau de protection conforme au RGPD.

Les transferts de données personnelles en dehors de l'Union Européenne sont encadrés par le RGPD, qui exige que ces données bénéficient d'une protection équivalente à celle offerte au sein de l'Union Européenne. Pour garantir ce niveau de protection, les responsables de traitement et les sous-traitants doivent évaluer le cadre juridique et les pratiques du pays destinataire des données avant d'en réaliser le transfert. Cette analyse est essentielle pour identifier et atténuer les risques liés à ces transferts, notamment par la mise en place de garanties supplémentaires.

Dans la continuité des recommandations du CEPD sur les mesures supplémentaires complétant les instruments de transferts, le guide de la CNIL propose ainsi une méthodologie non contraignante, en identifiant les étapes préalables à la réalisation d'une AITD ainsi que les étapes à suivre pour sa mise en œuvre, notamment la connaissance du transfert, l'identification de l'outil de transfert utilisé, l'évaluation de la législation et des pratiques du pays de destination, l'adoption de mesures supplémentaires si nécessaire, leur mise en œuvre et la réévaluation régulière du niveau de protection.

ACTUALITES DONNEES PERSONNELLES

Pas d'application de la clause exonératoire de responsabilité en cas de manquement à l'obligation d'information et de conseil

CA Paris, Pôle 5, chambre 11, 10/01/2025, RG n°22/11677

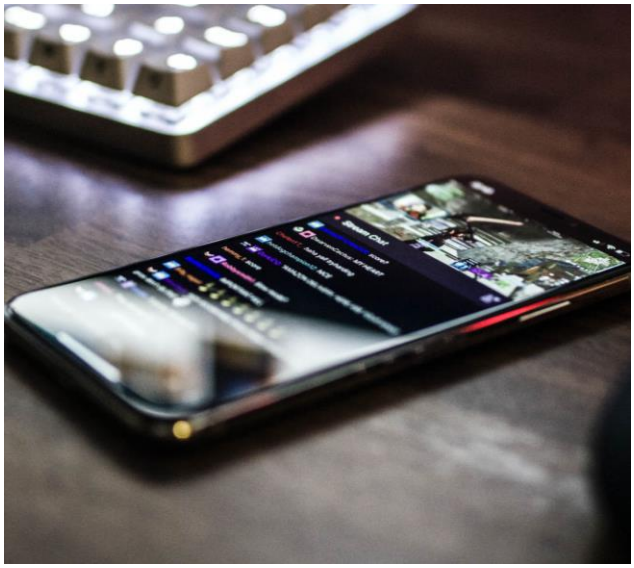
La Cour d'appel de Paris a rendu le 10 janvier 2025 un arrêt sur la question de l'application des clauses limitatives de responsabilité dans le cadre de la fourniture d'une solution logicielle.

En 2016, la société Payplug, s'est engagée à fournir à Wedoogift (nouvellement Glady), une interface de gestion des paiements incluant le dispositif "Smart 3-D secure" consistant à calculer en temps réel un score de risque associé à tout paiement visant à prévenir les opérations bancaires frauduleuses. En 2020, Wedoogift demande réparation pour les fraudes et le déblocage de fonds séquestrés. En 2022, le Tribunal de commerce de Paris condamne Payplug à verser des indemnités à Wedoogift.

En appel, Payplug invoque divers arguments, notamment le fait que la responsabilité en cas de fraude ne repose pas sur elle, qu'elle aurait respecté son devoir d'information et en tout état de cause, tente de s'appuyer sur la clause exonératoire de responsabilité acceptée par Wedoogift. Cette dernière quant à elle reproche à Payplug un manquement à son obligation d'information et de conseil, soutient que le système "Smart 3-D" n'était pas suffisamment sécurisé et demande réparation pour les fraudes subies.

La Cour d'appel confirme le jugement de première instance et rejette l'application de la clause exonératoire de responsabilité dès lors que la responsabilité de Payplug était engagée non pas pour une simple défaillance technique mais pour son manquement à son devoir d'information et de conseil. Ce comportement constituant une faute grave qui sort du champ d'application de la clause limitative, celle-ci ne peut exonérer un prestataire lorsqu'il néglige une obligation essentielle du contrat.

La Cour d'appel confirme ainsi le montant des dommages-intérêts fixé par le Tribunal de Commerce de Paris à 37.294,90 euros et condamne la société Payplug aux dépens et frais irrépétibles à hauteur de 5.000 euros.



ACTUALITES DONNEES PERSONNELLES

Adoption du Règlement sur l'Espace Européen des données de santé

Règlement sur l'Espace Européen des données de santé

Le 21 janvier 2025, le Conseil de l'Union européenne a adopté un règlement visant à faciliter l'échange et l'accès aux données de santé au sein de l'UE.

Cet Espace Européen des Données de Santé (EHDS) s'inscrit dans la « stratégie européenne pour les données » dévoilée en 2020, et constitue ainsi le premier de neuf espaces européens de données spécifiques à certains secteurs et domaines définis par la Commission.

D'une part, ce règlement vise à améliorer l'accès des individus à leurs données de santé. Les citoyens bénéficieront d'un accès plus rapide et plus aisé à leurs données de santé électroniques, qu'ils se trouvent dans leur pays d'origine ou dans un autre État membre. Ils disposeront également d'un meilleur contrôle sur l'utilisation de ces données. Les pays de l'UE seront tenus de mettre en place une autorité de santé numérique chargée de l'application des nouvelles dispositions.

D'autre part, ce texte vise à permettre la promotion de la réutilisation des données pour la recherche et l'innovation. L'EDHS offrira aux chercheurs un accès sécurisé à des types spécifiques de données de santé anonymisées et sécurisées, leur permettant ainsi d'exploiter le potentiel des données de santé de l'UE pour éclairer la recherche scientifique, développer de meilleurs traitements et améliorer les soins aux patients.

Le règlement vise également l'interopérabilité des systèmes de dossiers médicaux électroniques (DME) en exigeant que tous soient conformes aux spécifications du format européen d'échange des DME, tandis qu'actuellement le partage des données de santé entre les Etats membres est délicat en raison du niveau de numérisation variable d'un Etat à l'autre.

Le règlement sera formellement signé par le Conseil et le Parlement européen et entrera en vigueur vingt jours après sa publication au Journal officiel de l'Union européenne.

ACTUALITES DONNEES PERSONNELLES

Le CEPD élargit ses compétences

TUE, 29/01/2025, affaires jointes T-70/23, T-84/23 et T-111/23

Le 29 janvier 2025, le Tribunal de l'Union européenne a confirmé la compétence du Comité européen de la protection des données (CEPD) pour ordonner à une autorité de contrôle nationale d'élargir le champ de son enquête et de prendre de nouvelles décisions dans des affaires transfrontalières.

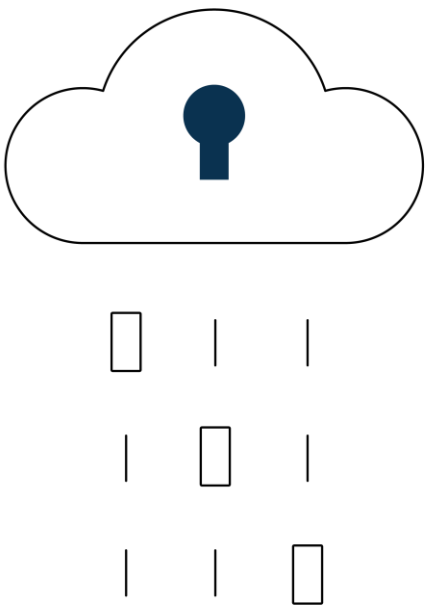
En 2018, des résidents d'Autriche, de Belgique et d'Allemagne ont déposé des plaintes contre Meta, alléguant des violations du règlement général sur la protection des données (RGPD) dans les applications Facebook, Instagram et WhatsApp, notamment une utilisation abusive des données personnelles pour la publicité ciblée sans consentement approprié. Le siège européen de Meta se trouvant en Irlande, la Commission irlandaise de protection des données (DPC) a été amenée à enquêter tant qu'autorité de contrôle chef de file, et a soumis des projets de décision aux autres autorités de contrôle concernées.

Aucun consensus n'ayant été trouvé à propos de ses projets de décisions, la DPC a saisi le CEPD dans le cadre du mécanisme de contrôle de la cohérence. Suite à l'examen de ces trois dossiers, le CEPD a approuvé sur le fond un certain nombre d'objections qu'il avait trouvé pertinentes et motivées mais n'a pas suivi la DPC dans son analyse selon laquelle l'utilisation des données pour les publicités ciblées était conforme au RGPD, sur la base de la notion de « performance d'un contrat ».

Le CEPD lui a donc demandé par le biais de trois décisions contraignantes de retirer dans ses décisions finales les constats liés à cette analyse, et plus globalement d'élargir son champ d'enquête et d'élaborer des projets de décisions complémentaires.

Contestant cette directive, la DPC a saisi le Tribunal de l'Union européenne, arguant que le CEPD avait outrepassé ses compétences. Dans cette décision, le Tribunal de l'Union européenne a cependant affirmé que le CEPD possède le pouvoir d'exiger des autorités nationales qu'elles élargissent leurs enquêtes et rendent de nouvelles décisions, conformément au droit de l'Union européenne.

Cette décision renforce le rôle du CEPD dans l'application cohérente du RGPD à travers l'Union européenne, tout en respectant l'autonomie opérationnelle des autorités nationales dans la conduite de leurs enquêtes. Elle souligne également l'importance d'une coopération efficace entre les autorités de protection des données pour assurer une application uniforme et efficace du RGPD.



Stéphanie Berland

Avocate - Associée

T: +33 1 40 69 26 63

E: s.berland@dwf.law

Emmanuel Durand

Avocat - Associé

T: +33 1 40 69 26 83

E: e.durand@dwf.law

Florence Karila

Avocate - Associée

T: +33 1 40 69 26 57

E: f.karila@dwf.law

Anne-Sylvie Vassenaix-Paxton

Avocate - Associée

T: +33 1 40 69 26 51

E: as.vassenaix-paxton@dwf.law

DWF est l'un des principaux fournisseurs mondiaux de services juridiques et commerciaux intégrés.

Notre approche de Gestion Juridique Intégrée offre une plus grande efficacité, une maîtrise des prix et une transparence pour nos clients.

Nous fournissons des services juridiques et commerciaux intégrés à l'échelle mondiale grâce à nos 3 offres, Legal Advisory, Legal Operations et Business Services, dans nos huit secteurs clés. Nous combinons de manière transparente un certain nombre de nos services pour fournir des solutions sur mesure à nos différents clients.

dwfgroup.com